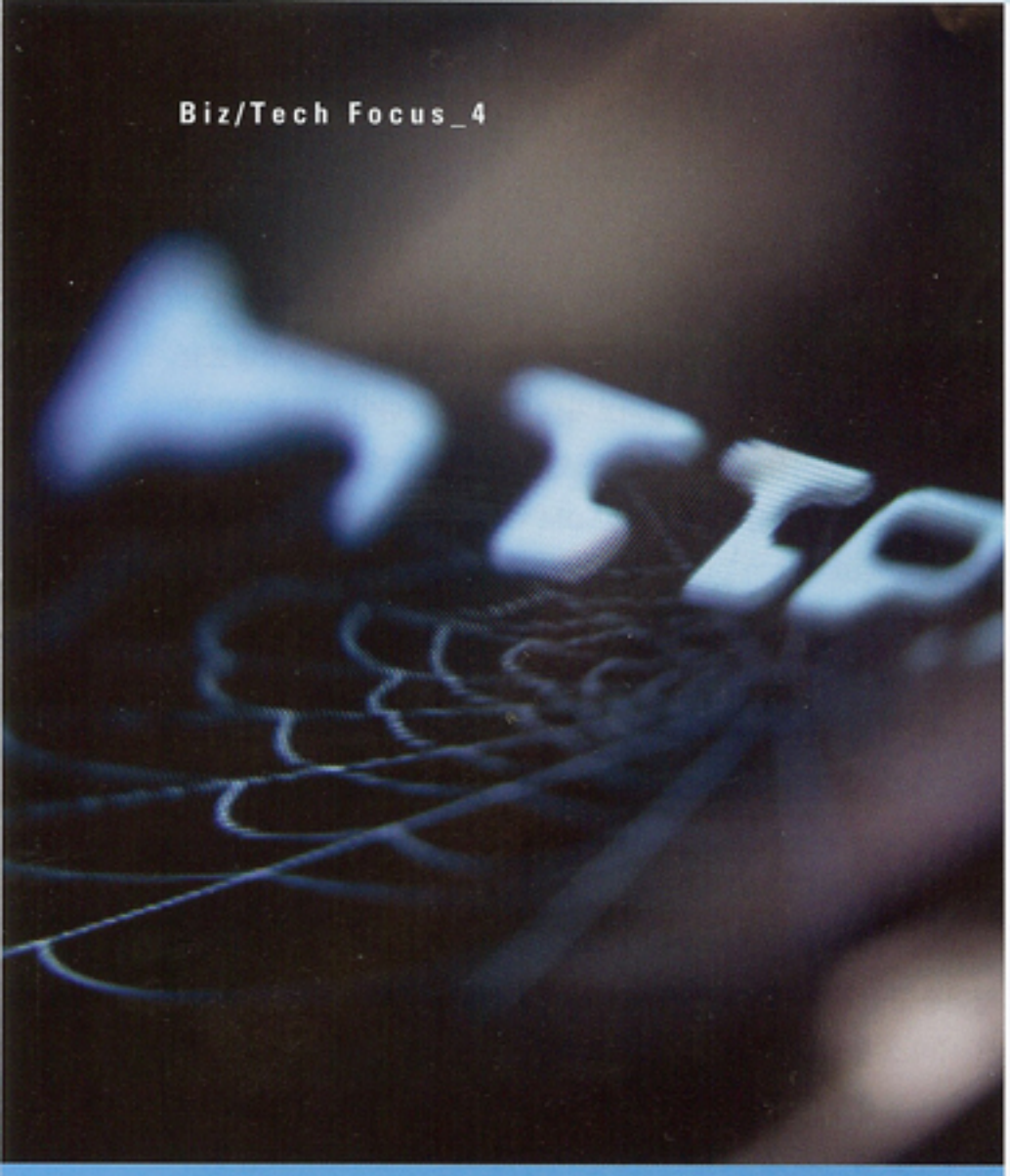


DDoS를 통한 네트워크 마비 협박과 공격 대응

DDoS 공격 막기 위한 기술 속속 발표...근본적인 방어는 어려워

〈연재순서〉

1. DDoS 공격과 대응기술
   - 서비스거부 공격의 유형 및 위치별 대응방안

2. 악성코드를 이용한 봇넷 공격
   - 봇넷의 심각성, 탐지 및 대응 방안

3. 조작된 패킷을 이용한 공격에 대응하기
   - IP 스푸핑 탐지 및 조작 패킷 공격 대응 방안

DDoS에 안전지대가 없다. 지난해 아이템거래 사이트를 공격해 DDoS의 위력을 보여준데 이어 올해는 미래에셋 등 금융권과 공공 · 민간을 가리지 않고 공격이 쏟아지고 있다. 공격양상도 없다. 아무데나 찔러봐서 돈이 나오면 좋고 안 나오면 말고의 식이다. 본지는 지난 2000년부터 DDoS의 위험성을 알리고, 대응기술에 대한 연구를 해 온 고려대학교 정보통신대학 컴퓨터보안연구실과 함께 'DDoS를 통한 네트워크 마비 협박과 공격 대응방법' 을 총 3회에 걸쳐 연재한다.

이희조 고려대학교 교수(heejo@korea.ac.kr)

분산 서비스 거부 공격
(DDoS: Distributed Denial of Service)

2008년 3월 21일 오후 미래에셋그룹 홈페이지가 중국 크래커에 의해 DDoS 공격을 당해 서비스 장애가 발생했다. 막대한 트래픽이 전달돼 정상 사용자가 홈페이지에 접속할 수 없었으며, 이 과정에서 중국 크래커들은 네트워크를 마비시키지 않는다는 조건으로 5000만원을 요구했다. 이러한 DDoS 공격자들은 시스템 내부 정보에는 관심이 없다. 개인정보를 유출하고 중요 기업정보를 빼내는 것이 아니라 웹 서버나 네트워크를 마비시키겠다고 위협하고 이를 풀어주는 대가로 돈을 요구한다.

지난해 게임 아이템 거래 사이트인 아이템베이와 몇몇 업체들이 DDoS 공격으로 인해 서비스 장애가 발생해 막대한 손실을 입은바 있다. 이러한 공격이 상거래나 금융 사이트에서 발생한다면 막대한 손실을 본다는 사실은 불에 보듯 뻔한 이야기 이다. 또한 고객의 손실에 대한 피해보상, 나아가 회사의 이미지 실추까지 감안한다면, 회사의 손실은 복구가 불가능할 지경에 이를 수도 있다.

서비스거부공격(DoS: Denial of Service)은 정상적인 사용자가 서비스를 이용하지 못하도록 방해하는 공격 기법이다. 예를 들어 서버나 네트워크에 조작된 패킷을 반복적으로 보내 정상 트래픽이 처리되는 것을 방해하거나 두 기기의 통신 연결을 방해하는 등의 시도를 하는 것이 DoS 공격이다. 그러나 컴퓨터와 인터넷 환경의 급속한 발전으로 소규

모의 DoS 공격으로는 서버나 네트워크를 무력화시키기에 부족함이 많았다. 최근에는 DoS 공격을 극대화시키기 위해서 수 천, 수 만대에 이르는 다수의 컴퓨터를 동원하여 공격을 감행하는 DDoS(Distributed Denial-of-service) 공격이 인터넷을 위협하는 이슈로 부상했다. 실제 공격이 처음으로 나타난 것은 1999년 이전 이었으나 큰 주목을 받게 된 것은 2000년 2월 Yahoo, Buy.com, e-bay, Amazon, E-Trade, CNN등 유명 인터넷 사이트가 공격을 받아 몇 시간 동안 접속할 수 없었던 사건이 발생한 다음부터이다.

〈그림1〉DDoS 공격의 동향

DDoS 공격이 가능한 것은 현재 인터넷 설계가 정보를 주고받는 두 개체(서버와 클라이언트)가 트래픽을 감시하거나 조정하는 것 보다 네트워크에서 정보전달이 원활하고 빠르게 이뤄질 수 있도록 제공하는데 초점을 맞췄기 때문이라고 볼 수 있다. 따라서 정보를 보내는 송신자 측에서 정보를 받는 수신자 측이 처리를 할 수 없을 정도로 과다한 정보를 전달하면, 수신자 측에서 과다한 정보를 처리하지 못하고 둘 사이에 정보 전달이 원활하게 이루어 질 수 없으며, 이러한 상황을 악의적인 목적으로 발생시키는 공격이 바로 DDoS 공격이다.

정보전달을 빠르게 하기위한 인터넷 설계의 취약점 중 DDoS 공격의 기회를 만드는 요소가 몇 가지 있다. 인터넷에 산재해 있는 수많은 컴퓨터들이 모두 완벽하게 보안적인 대비를 하는 것은 불가능하다. 일부 컴퓨터의 보안을 완벽하게 한다고 해도 보안이 취약한 수많은 컴퓨터가 인터넷에 산재해 있기 때문에 이들이 공격에 이용될 수 있다. 또 각각 인터넷 개체들이 가지고 있는 한정된 자원을 많은 서비스 사용자들이 사용한다는 점, 인터넷을 이루고 있는 각각의 네트워크들을 서로 다른 정책에 의해 운영하고 있어 모든 네트워크들을 강제적으로 통제해야 하는 방어 대책들이 현실적으로 힘들다는 점들 또한 DDoS 공격이 급증하는 이유라고 할 수 있다.

DDoS 공격 동향

작년 한 해 동안 DDoS 공격은 커다란 이슈였다. 2007년 1월부터 2008년 3월까지 국내의 개인이나 회사들에게 인터넷 접속 서비스, 웹 호스팅 등을 제공하는 회사인 ISP(Internet Service Provider)의 일부 구간에서 수집된 공격 유형을 분석한 결과, DDoS 공격 트래픽이 많이 탐지 되었다는 사실이 이를 방증한다. 또 DDoS 공격에 악용되는 것으로 알려진 'Virut' 바이러스에 대한 피해 신고가 2007년 7월부터 9월 사이에 1, 2위를 꾸준히 차지하기도 했다.

DDoS 공격이 기업에 미치는 악영향은 엄청나다. 네트워크가 완전히 다운되는 사태가 벌어지지 않더라도, 단지 인터넷 서비스 속도가 갑자기 느려지거나 불안정하게 되는 것만으로도 엄청난 피해를 입을 수 있다. 하루 중 언제라도 필요에 의해 서비스를 이용하기 위해 접속하는 많은 고객들이 불만족스러운 서비스로 경쟁사로 이동할 수 있고, 서비스수준협약(SLA: Service Level Agreement)에 위배돼 막대한 규모의 금전적인 피해보상을 하는 경우도 있다. 대규모의 집단소송에 휘말릴 가능성도 있고, 이로 인한 기업 이미지 실추, 주가하락, 매출감소 등 예상할 수 있는 피해조차도 막심하다.

기업환경에서 모든 피해는 금전적인 손실로 귀결된다. DDoS로 인한 금전적인 피해는 어느 정도일까? 포레스트, IDC 등 여러 시장조사 기관에서 집계한 객관적인 통계 수치에 따르면, 예를 들어 시스코 정도의 대규모 글로벌 기업이 24시간 동안 서비스 마비 상황에 이르렀을 때 약 3000만 달러(313억 원)의 직접적인 손실이 발생한다고 추정된다. 또 다른 세계적인 시장 조사 기관인 양키 그룹의 집계에 의하면 2000년 2월에 발생했던 인터넷 사이트에 대한 대규모의 DDoS 공격에 의한 직접적인 피해 액수는 12억 달러(약 1조2500억 원)에 이른다고 발표했다. 2001년 1월에 마이크로소프트사의 인터넷 사이트가 수일 동안 DDoS 공격을 받았을 때 발생했던 손실 규모는 5억 달러(약 5200억 원)로 집계됐다.

DDoS 공격은 과거에는 자기과시나 영웅심리에 의해 특정 대형 웹사이트를 공격했으나 최근에는 중소형 사이트를 포함, 금전을 갈취하는 협박형(ransom) 공격으로 바뀌는 양상을 보이고 있다. 지난해 국가·민간 부문의 사이버침해 위협과 관련한 10대 동향 이슈 중 DDoS 공격이 첫 번째 이슈가 될 정도로 중대한 위협 요소로 평가 되었으며, 2007년 들어 중국인으로 추정되는 해커가 국내 특정 웹 사이트에 대해 메신저나 이메일, 전화를 통하여 금품을 요구하고, 이에 응하지 않을 경우 DDoS공격을 가하는 등 협박형 DDoS 공격이 크게 증가했다.

공격대상은 수사의뢰를 꺼려할 것으로 보이는 불법 성인사이트에서부터 온라인 게임아이템 거래사이트, 온라인 펜션 예약사이트 등으로 다양화되었고 공격트래픽의 규모도 수~수십 Gbps에 달하여 국내 인터넷에 커다란 위협으로 대두되고 있다.

하지만 이런 협박성 DDoS 공격 이외에 다른 형태의 공격도 존재했다. 2007년 6월 〈Czech Business Weekly〉 지에 실린 한 기사에 따르면 에스토니아가 1991년 소련에서 독립한 후 2007년 4월에 수도에 서 있던 '붉은 군대 병사' 동상을 끌어내렸고 이로 인해 에스토니아에 있던 소수계층의 러시아 사람들이 커다란 폭동을 일으켰다. 그 후 5월에 에스토니아의 정부, 정당, 신문사, 은행, 기업들의 웹사이트가 2주간 다운

되는 사태가 발생했고 이 때 에스토니아의 웹 사이트들을 공격한 해커들이 사용한 기법이 바로 DDoS 공격이었다. 에스토니아에서는 공격 패킷 중 하나가 러시아의 푸틴 대통령의 측근의 IP 주소를 가지고 있었다고 주장했지만 러시아 정부는 부인했고 러시아의 개입에 대한 증거를 찾을 수는 없었다.

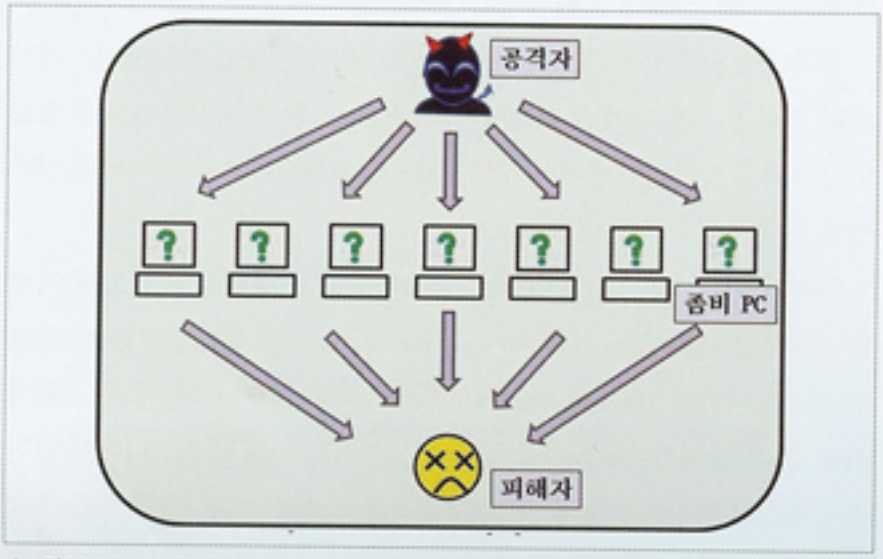
최근에 이와 비슷한 사례가 한 번 더 있었다. 2008년 4월 26일 몇몇 RFE(Radio Free Europe)의 웹 사이트들이 DDoS 공격을 받았다. RFE는 미국 의회로부터 재정적인 지원을 받는 언론 기관이다. 공격이 한창 최고조였을 때 RFE 사이트에 5만개 이상의 접속 요청 메시지들이 보내졌다. 이 날은 체르노빌 원자력 발전 사고 22주년을 맞는 날이었기에 벨로루시 정부가 계획 중인 원자력 발전소 건설에 대해서 항의하는 가두 행진이 있었다. 이 사건 역시 공격의 근원지는 알 수 없지만 그에 대해서 RFE의 온라인 방송을 막으려는 벨로루시 측의 공격이 아니었을지 추측만이 가능할 뿐이다.

이와 같은 사례는 DDoS 공격이 협박성 금품 갈취 공격으로 악용되는 것 외에도 국가간의, 혹은 다수 집단간의 정치적 목적으로 사용될 수도 있음을 보여준다. 이런 경우에 있을 피해 규모를 생각해 본다면 정말로 엄청난 규모가 아닐 수 없다는 것을 알 수 있다.

DDoS 공격 단계

DDoS 공격을 하기 위해서 몇 단계 과정을 수행해야 한다. 공격자가 처음으로 해야 할 일은 여러 개의 기계들을 선택하는 일이다. 이 과정은 보통 보안 취약점들이 있는 원거리 기계들을 탐색해 이를 감염시키며 봇 등을 통해 자동화한다. 예를 들어 공격자가 취약점을 가진 컴퓨터들을 감염시키는 코드에 인접한 컴퓨터 중 동일한 취약점을 가진 컴퓨터를 탐색해 감염 시키는 또 다른 코드를 삽입해두었다면, 감염된 컴퓨터는 감염 후 2차적으로 다른 컴퓨터를 감염시키는 행위를 하게 된다. 그리고 감염된 기계들은 새로운 기계들을 찾는데 사용된다.

또 다른 방법은 네티즌들이 많이 찾는 유용한 소프트웨어를 가장해 공격 소프트웨어를 분산시키는 것이다. 공개자료실이나 P2P 사이트, 이메일 등을 이용해 악성코드에 감염된 첨부파일을 보내며, 이 공격을 통해 감염된 기계는 또 다시 공격 패킷을 보내는데 사용된다. 공격자들은 공격 중에 종종 패킷의 송신 측 IP주소를 조작해 감염된 기계의 정체를 숨긴다. 하지만 그것은 DDoS 공격이나 좀비 PC들이 탐색되지 않도록 하는 것뿐이고, 공격의 성공 여부와는 관계없다.



〈그림2〉DDoS 공격의 구조

DDoS 공격은 다음과 같이 여러 가지 기준을 통해서 분류할 수 있다.

첫째, 공격의 자동화 정도에 따라서 분류가 가능하다. 위의 여러 단계 중에서 취약한 호스트를 탐색하고 감염시키는 단계를 자동화할 수 있다. 유명한 Code Red(CRv2)는 임의 탐색을 수행한 것으로 알려져 있다. 임의 탐색은 웜이 스스로 전파되기 위해 IP 주소 공간에서 임의의 IP 주소를 선택하는 방식이다. Code Red II와 Nimda 웜 같은 경우 로컬 서브넷 탐색 방식을 이용했는데 이 방법을 이용하면 단 한 개의 탐색 프로그램의 복사본이 방화벽 뒤의 취약한 많은 호스트들을 감염시킬 수 있다.

둘째, 서비스를 거부하는데 이용되는 약점에 따른 방법이 존재한다. 한 가지 방식은 취약점 자체를 이용하는 방식으로 공격대상에 존재하는 취약점을 악용한다. 예를 들어 한 PC가 다른 PC와 통신 하고자 하는 다수의 메시지를 보내기만 하고 종료 시키지 않는다면 이 때 메시지를 수신하는 PC 자원을 고갈시킬 수 있다. 또 다른 방법으로는 트래픽 플러딩 공격이 있다. 이는 과도한 양의 패킷을 수신 측에 전송해 수신 측 PC에 패킷이 범람, 다른 서비스를 할 수 없는 상태가 되도록 만드는 방법이다.

셋째, 위에서 잠시 언급한 것처럼 패킷을 보낼 때 패킷의 송신 측 IP 주소를 입력하는 곳에 들어갈 정보를 조작해 마치 다른 곳에서부터 패킷이 보내진 듯 보이게 하는 IP 스푸핑 방식에 따른 분류가 가능하다. 특히 IP 스푸핑은 '분산 공격' 에서 한 걸음 더 나아가 '반사 공격' (reflection attack)을 하기 위해 사용되기도 한다. 일반적으로 A, B, C 세 개의 PC가 있을 때, A가 어떤 패킷을 C로 보내면 C는 그 패킷에 대한 응답을 당연히 A에게 전송한다. 하지만 '반사 공격' 의 경우에는 A가 어떤 패킷을 B의 주소로부터 보내지는 것으로 패킷을 수정해 C에게 전송하면 C는 패킷을 받고 응답을 하기 위한 패킷을 A가 아닌 B에게 보내게 될 것이라는 점을 이용한 공격이다. 위의 상황에서 A가 단지 한 개의 패킷을 브로드캐스팅하는 것만으로도 그 메시지를 받은 수많은 PC들은 B에게 응답을 하게 되어 B가 DDoS 상황에 놓이게 된다.

이외에도 감염된 좀비 PC들이 공격 패킷을 보내는 비율이 일정한가, 변하는가에 따른 분류, 공격의 특징이 존재하는가에 따른 분류 등 여러 가지 기준에 따라서 DDoS 공격을 분류할 수 있다.

DDoS 공격의 방어

다른 모든 공격들과 마찬가지로 DDoS 공격 또한 탐지를 피하거나 어렵게 만드는 방법들이 계속해서 발전하고 있다. 그리고 DDoS 공격에 대한 탐지에 성공한다 하더라도 더 큰 과제는 DDoS 공격 하에서 DDoS 공격에 이용되는 패킷과 정상적인 사용자의 패킷을 구별해 내기가 쉽지

않다는 점이다. 그렇다면 DDoS 공격에 대한 대처는 어떻게 이루어져야 할까.

DDoS 공격에 효과적으로 대응하기 위해서는 네트워크 보안을 위해 네트워크 침임을 탐지하는 시스템이나 방어 기술을 적용할 필요성이 있다. 실제로 최근 DDoS 공격으로 피해를 입은 업체들은 대부분 IPS, 방화벽 등 기본적인 보안 솔루션을 갖추지 않은 경우가 대부분이었다. 방어 솔루션 또한 방어 기술에 대한 연구가 선행되어야만 가능할 것이다. DDoS 공격에 대한 방어 기술에는 공격을 조기에 예방하거나 탐지하는 방식이 있다.

첫 번째로 조기 예방을 목표로 하는 작업 중에는 실제로 통신에 쓰이는 시스템이나 프로토콜의 원천적인 취약점들이 공격에 사용될 수 없도록 직접적으로 보완하는 방법이 있다. 예를 들어 TCP 패킷을 이용한 많은 공격 방법들이나 OS 자체의 버그를 이용한 공격을 막기 위해 보완되는 패치가 있을 수 있다. 그리고 프로세스, IP주소 등이 사용하는 서버의 자원을 시스템이 지속적으로 감시하여 정상적으로 자원을 사용하는 사용자에게만 자원을 할당하는 기술도 존재한다.

두 번째 DDoS 공격의 탐지 방법으로 일정한 패턴을 분석해 데이터베이스에 저장하고 연결돼 있는 통신을 관찰해 그 중 한 패턴과 같은 행위를 하는 통신 연결을 차단하는 방법이 있다. 그리고 평소의 정상적인 트래픽을 관찰하여 모델링하고 그 결과와 다른 이상 징후를 보일 때를 포착해 공격을 탐지하는 방법 등이 연구되고 있다. 이 외에도 요즘 몇몇 웹사이트들에서 종종 볼 수 있는 방식으로 그림에 적힌 글자, 혹은 숫자를 따로 입력하도록 유도하는 화면 또한 자동화된 DDoS 공격을 막기 위해 고안된 기술이다.

하지만 이렇게 연구되고 있는 기술만으로 다양한 공격을 막아낼 수 없다. DDoS 공격을 막아내기 위해서는 체계적이고 순차적인 방어체제의 구성 및 ISP나 IDC 등 여러 기관 간의 공조 체제가 필수적이다.

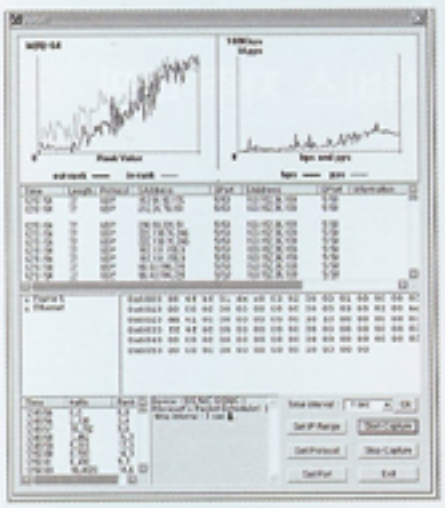
우선 공격에 효과적으로 대응하기 위해 공격의 탐지, 공격 방법의 분석 및 인지, 필터링 룰 적용 등의 체계적이고 자동화된 시스템의 구축이 필요하다. 예를 들어 어떤 서버의 자원이 고갈되기 시작하면 관리자는 이에 대응하기 위해 현재 수신하고 있는 트래픽의 특성을 분석한다. 그 결과 SYN 플러딩 공격을 받고 있다고 판단하면 SYN 과 SYN/ACK의 매칭을 통해 서버에서는 SYN만 송신하는 클라이언트들을 차단하는 룰을 서버에 적용하는 등의 시나리오가 존재할 수 있다. 그러나 이렇게 서버에서 공격을 막아내기 위해 아무리 룰을 생성하고 적용하는 등의 순차적인 방어 시스템을 구축한다고 하더라도 IP 스푸핑과 같은 공격에는 결국 서버 측에서는 공격을 막아내기가 쉽지 않을뿐더러 대부분의 DDoS 공격에 쓰이는 수 많은 패킷들이 서로 다른 ISP들을 통해 유입되기 때문에 ISP와 IDC의 공조를 통해 트래픽이 유입되는 소스부분에서 원천적으로 막아내야 할 필요성이 있다.

고려대학교 정보통신대학 컴퓨터보안연구실에서도 현재 DDoS 공격의 방어에 대한 연구가 진행 중에 있다. 특히 최근에는 DDoS 공격의 트래픽과 정상적인 서비스 이용자의 접속 폭주 트래픽을 랜덤성을 이용해 서로 구별해 내는 것을 주제로 한 연구가 진행 중에 있다.

또한 전송률 제한(Rate-limiting) 기법을 이용해 개인 컴퓨터나 액세스 망 단에서 밖으로 나가는 패킷의 양을 조절하는 연구도 있었다. 이 연구는 악성코드에 감염된 일반 사용자의 컴퓨터에서 자신도 모르는 사이에 DDoS 공격 트래픽을 전송할 수 있다는 점을 바탕으로 사용자의 컴퓨터가 DDoS 공격의 특성을 보이는지 여부를 4단계로 나누어 검사하고 공격 근원지에서 패킷 전송량을 조절하는 방어 기법이다.

이외에 IP 스푸핑을 탐지하는 기술로, BASE라는 연구를 미국 CMU 대학과 함께 공동연구를 진행하고 있으며, 이는 패킷에 정보를 표시해 정상적이지 않은 패킷을 구분해 필터링하는 방식이다. 그 밖에 인터넷의 공격을 시각적으로 표현해 주는 공격 시각화 기법 PCAV (parallel coordinate attack visualization)의 연구를 진행했으며, PCAV는 웜, 스캐닝, DDoS 등의 주요 인터넷 공격들을 탐지하기 위한 실시간 시각화 시스템에 관한 연구이다. 〈그림3〉과 〈그림 4〉는 이러한 기술을 이용해 탐지해 낸 상황을 보여주고 있다.

〈그림3〉 공격 시각화 도구인 PCAV를 이용한 DDoS 공격 탐지



〈그림4〉 웜의 조기탐지를 이용해 DDoS에 사용되는 컴퓨터들의 감염을 사전에 방지함으로써DDoS 공격에 대한 원천적인 봉쇄

많은 DDoS 공격 방어법들이 인터넷이라는 하나의 집단에 있어서 개개인에 각자 적용 가능한 것이 아니라 서로 협조가 필요한 방법들이기 때문에 현실적으로 실현 가능성이 그렇게 높지는 않다. 하지만 현재 DDoS 공격으로 인한 피해가 계속 증가하고 있어 앞으로는 여러 기관들의 협조가 요구된다.

DDoS 공격은 지금까지의 공격들과는 다르게 정보의 유출 혹은 변조가 아니라 서비스의 이용 자체를 막는다는 목적을 가지고 있다. 그리고 이러한 목적과 현재의 인터넷의 구조상 DDoS 공격은 너무나도 잘 맞아떨어지는 공격법이라고 보여진다. 그렇기에 방어가 어려운 점 또한 사실이다. 하지만 우선은 할 수 있는 방어에 최선을 다하고 그래도 혹여 피해를 입은 기관들은 정보 보호 관련 기관에 해당 사실을 알려 정보를 공유하고 각 연구 기관들은 해당 정보를 바탕으로 DDoS 공격의 방어법에 대한 연구에 더욱 박차를 가해야 할 것이다.